F5 Cloud Federation リファレンス・アーキテクチャ

分散 SaaS プロバイダ・アイデンティティの欠点を排除し、
管理システムにアクセスしてセキュリティを強化

Technical White Paper

目次

はじめに 3

ビジネス上の課題 3
- SaaSの採用 3
- テクノロジサイロ 4

ビジネス・ソリューション 6

テクノロジ・ソリューション 6

ビジネスメリット 7

まとめ 8

はじめに

多数の組織が、社内ソリューションを導入して維持する代わりに、クラウドベースのサービスを採用するメリットを認識するようになっています。サービスとしてのソフトウェア（SaaS）プロバイダは、すぐに使用できる、サブスクリプション・ベースのモデルを使用して、コスト効率の高いマルチテナントの環境でニッチな専門知識を配信できます。ただし、SaaS オプションのメリットによって、最新のアクセス制御や信頼性のあるセキュリティ・ポリシー・エンフォースメントが犠牲になることもよくあります。社内管理のサービス同様、SaaS プロバイダはユーザ名、パスワード、アクセス制御の実行のために、独自の識別およびアクセス管理（IAM）システムを維持しているため、IAM サイロとセキュリティ管理の問題が生じ、複数の IAM システムの使用による共時性と統合の欠如に至ることになります。

IAM サイロにより、セキュリティが損なわれ、生産性が低下する可能性が生じます。

- セキュリティリスクはパスワード疲労や、さらに重要な期限切れアカウント削除の遅れによってもたらされます。
- 生産性の低下は、新入社員や請負業者のための新規ユーザアカウント作成の遅延や、多数の IAM システムで求められる管理費用が原因です。

F5® Cloud Federation は、社内で維持される IAM システムと外部サービスとの間のこのような SaaS の欠点を排除することで、どこでも一貫性のあるセキュリティが達成できます。

パスワード疲労

「同じユーザIDとパスワードを使用すると、アカウントをハッキングの危険にさらすことになり、複雑なパスワードを選択すれば、すべてを記憶するのが難しくなる。どこかの時点で管理しきれなくなる。これがパスワード疲労だ」。

-TriCipherマーケティング担当副社長
ジョン·ブロディ

ビジネス上の課題

SaaS の採用

SaaS は企業にとってメリットが多いため、市場はユビキタスで急速に成長しています。

- SaaS はクラウドベースであるため、取得、インストール、メンテナンスが必要なテクノロジはありません。
- SaaS は IT リソースを解放し、より戦略的なプロジェクトに集中できます。
- SaaS は、通常、どのデバイスからでも、どこからでも利用可能なサービスでモビリティを支援します。
- SaaS はサブスクリプション・ベースで、社内に持ち込まれる既製のソフトウェアよりライセンスコストが単純です。

それでも、SaaS はプライベートに維持され、セキュリティ保護されているリソースにとっては外部にある追加サービスであり、この追加サービスを使用することで、新たな独自の課題が発生します。

テクノロジサイロ

組織外（プライベート·データ·センタ外）から配信されるサービスは、本質的に、データ管理、アプリケーション·セキュリティ、識別とアクセス管理に関するテクノロジサイロを表します。

SaaS では、データ管理とアプリケーション·セキュリティは SaaS プロバイダの管理下にあり、これは簡単に変更できるものではありません。その理由は、SaaS に由来するメリットの大多数は、サービスデリバリの複雑さはサービス自体を使用することによるものだという単純な事実です。したがって、データ管理とアプリケーション · セキュリティを契約者に公開するということは、本来の SaaS をサービスとしてのインフラストラクチャ（IaaS）に変換することであり、管理をサービスユーザの管理下に戻すことで、SaaS のメリットすべてを即座に失うことになります。本質的に、SaaS を選択するということは、プロバイダのデータ管理ポリシーとアプリケーション · セキュリティ · ポリシーを受け入れ、そのポリシーへの信頼を確立するということを意味します。

識別とアクセス管理に関して言えば、SaaS プロバイダは独自のソリューションを提供しており、契約者の社内 IAM システムに加えて、情報を入力して維持するのは契約者次第であり、ここでも孤立したシステムと IAM サイロが生じることになります。この IAM サイロの増加により、次のように新たなリスクが発生します。

- データ保護
- 生産性
- セキュリティの整合性

データ保護

データ保護は重要であり、組織は外部プロバイダに委託したデータの窃盗を非常に（これには正当な理由がありますが）恐れていて、SaaS プロバイダも例外ではありません。ただし、すべての IAM サイロで従業員が管理するパスワードを追加すると、弱いパスワードによってデータの窃盗攻撃が容易になるため、リスクは拡大します。しかしながら、オンラインの信用調査会社 Experian による 2012 年のレポートでは「平均して 26 の異なるオンラインアカウントに対して、ユーザは異なるパスワードを 5 つしか使用していなかった」のです。

「同じユーザ ID とパスワードを使用すると、アカウントをハッキングの危険にさらすことになり、複雑なパスワードを選択すれば、すべてを記憶するのが難しくなる。どこかの時点で管理しきれなくなる。これがパスワード疲労だ」とTriCipherマーケティング担当副社長ジョン · ブロディは「*Forbes Magazine*」の 2009 年版で説明しています。

パスワードの強度やハッキングの問題よりさらに重要なのは、元従業員や請負業者のユーザアカウントの削除が遅れることによるデータ保護セキュリティへの影響です。人事システムはすべての IAM サイロ全体の相互参照をどのくらいの頻度で行っているのでしょうか。承認に関する変更と、その変更が IAM サイロ全体に反映されるまでの時間とのギャップで、深刻なセキュリティ違反が生じます。しかしながら、熟練した IT リソースはすでに需要が高いため、削除の遅れは避けられません。

生産性

新入社員や請負業者が必要なシステムにアクセスして稼働できるまでの遅れは、生産性に無視できないほどのコストを生じさせます。新しい個人アクセスをプロビジョニングするまでにかかる時間は関与するテクノロジサイロの数によって増加するため、組織が SaaS のメリットをより多く活用すればするほど、より多くのアクセスのプロビジョニングが必要になります。

セキュリティの整合性

組織はアクセス技術を調査して、プライベートに維持しているシステムに適切な認証ソリューションと承認ソリューションを選択するために多大な時間と資金を投資しています。主要なソリューションは多要素認証で、要素はユーザ名、パスワード、ワンタイムパスワードまたはコードなど、別の形態の認証チャレンジで構成されることがよくあります。このようなソリューションの例として次のようなものが挙げられます。

- RSA SecureID
- Google Authenticator
- Entrust

このような追加レベルのセキュリティは人気が高まっており、たとえば、ワンタイムパスワードなどは書き留めることができないため、パスワード疲労に由来するセキュリティ上の欠陥への対処に役立ちます。ワンタイムパスワードは 1 回限り有効で、その後は期限切れになります。

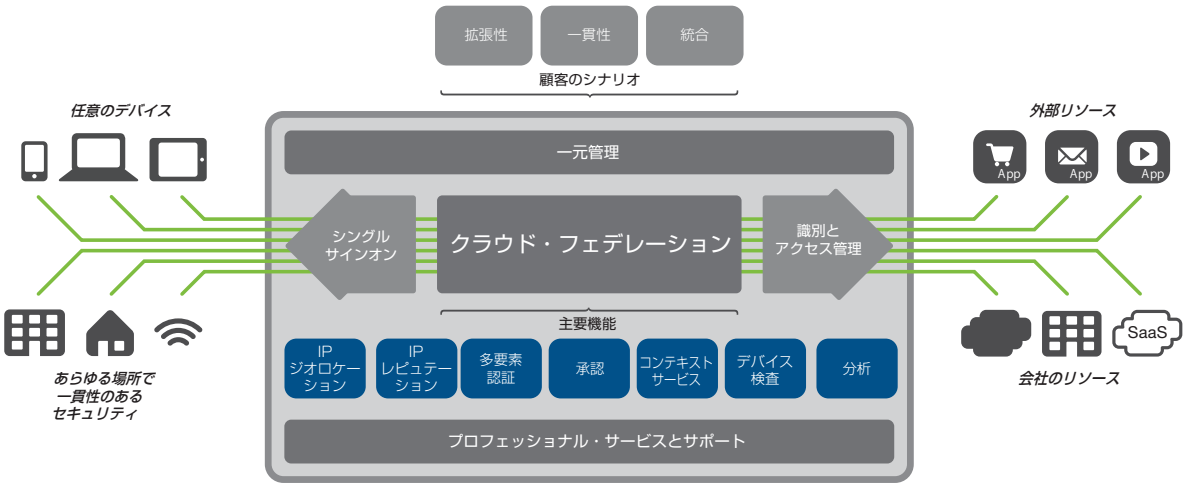
このようなソリューションは内部管理のシステムには実装できる可能性がありますが、SaaS プロバイダから多要素認証をすぐには利用できません。もしできたとしても、別個管理の 2 要素認証となり、セキュリティは強化されますが、やはり IAM サイロが生じます。

Forrester Research は、2022 年には IT 部門が消滅すると予測

Forrester Research が 1,000 名の IT 専門家を対象に実施した最近の調査によると、IT 専門家は人事や顧客関係管理など、ミッションクリティカルでないアプリケーションのオフロード管理にホスト型（SaaS）製品を利用するようになっていることがわかっています。サブスクリプション・ベースの SaaS 価格モデルは、IT 予算費用もパッケージ化されたソフトウェアや自社のソフトウェアと同等以下に抑えることができます。

ビジネス・ソリューション

SaaS 契約者は、別の方法で SaaS プロバイダのサイロ化した IAM ソリューションの採用と管理を行うことができます。組織は IAM フェデレーションを実装して、SaaS プロバイダのサービスと契約者が所有して契約者が管理する IAM 技術との間に信頼関係を構築することもできます。ただし、このようなソリューションを実現するには、アーキテクチャや管理をより複雑にしたり、中断して技術を統合したりせずに、プロバイダと契約者との間に新たなネットワークを構築、維持して達成する必要があります。



F5 Cloud Federation ソリューション

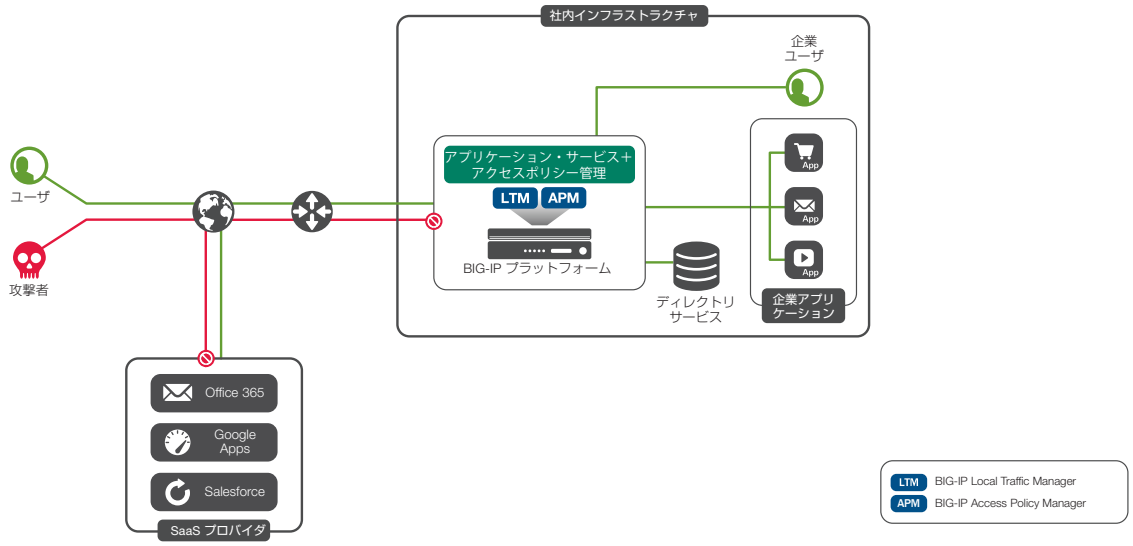
テクノロジ・ソリューション

F5 Cloud Federation アーキテクチャは両方の要件を満たします。関係者間の認証データと承認データのやり取りに XML ベースの公開標準データ形式である Security Assertion Markup Language（SAML）を使用しています。SAML テクノロジでは、SaaS プロバイダを超えて個々のユーザアカウントを管理する必要がありません。SAML が対応する最も重要な要素は、Web ブラウザのシングルサインオン（SSO）です。

さらに、F5 Cloud Federation アーキテクチャでは、2 要素認証、IP ジオロケーションの実行とデバイスの検査など、より強力な承認ソリューションの導入が可能になります。

F5 BIG-IP® Local Traffic Manager ™（LTM）と BIG-IP® Access Policy Manager®（APM）を併用することで、以下に必要なプラットフォームを提供します。

- 組織のプライベート IAM システムと外部 SaaS プロバイダとの間の SAML 通信
- BIG-IP を使用してアクセスするすべてのシステムに関するすべてのユーザに対する一貫性のある多要素認証



F5 Cloud Federation アーキテクチャ

ビジネス上のメリット

F5 Cloud Federation アーキテクチャを実装することで、組織は以下を実現できます。

- SaaS アプリケーション全体で SSO を実装して、パスワード疲労の原因を削減
- すべてのシステムで一貫性のあるセキュリティポリシーを実行
- アクセスアカウントへの権限付与と削除のための管理コストの削減
- 複雑さの削減と生産性の向上
- SaaS のメリットへの投資とセキュリティリスクのより適切な管理

まとめ

孤立したシステムをテクノロジサイロとして運用すると生産性とセキュリティを大きく阻害します。組織の業務上のニーズへの迅速な対応能力を制限し、実績と信頼のあるセキュリティポリシーを損ないます。F5 Cloud Federation アーキテクチャでは、SaaS アクセスサイロを削減してセキュリティを強化し、生産性を向上し、SaaS モデルを安全に採用できます。

F5 ネットワークスジャパン株式会社

東京本社
〒107-0052 東京都港区赤坂 4-15-1 赤坂ガーデンシティ 19 階
TEL 03-5114-3210 FAX 03-5114-3201

西日本支社
〒530-0012 大阪府大阪市北区芝田 1-1-4 阪急ターミナルビル 16 階
TEL 06-7222-3731 FAX 06-7222-3838

www.f5networks.co.jp

WP-CLOUD-10855-cloud-federation 1013